



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

JW

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/938,489	08/27/2001	James Malcolm Vignoles	550-261	2875
7590	04/05/2005		EXAMINER	
NIXON & VANDERHYE P.C. 1100 North Glebe Road, 8th Floor Arlington, VA 22201-4714			SCHUBERT, KEVIN R	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	09/938,489	VIGNOLES, JAMES MALCOLM
	<b>Examiner</b> Kevin Schubert	<b>Art Unit</b> 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 27 August 2001.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-36 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 15 November 2001 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s). (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_
- 4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_

Art Unit: 2137

## DETAILED ACTION

Claims 1-36 have been considered.

### ***Claim Objections***

5        Claims 12,24, and 36 are objected to because of the following informalities: "detects" should be  
"detect". Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness  
10 rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set  
forth in section 102 of this title, if the differences between the subject matter sought to be patented and  
the prior art are such that the subject matter as a whole would have been obvious at the time the  
invention was made to a person having ordinary skill in the art to which said subject matter pertains.  
15        Patentability shall not be negated by the manner in which the invention was made.

Claims 1-6,8-9,11-18,20-21,23-30,32-33, and 35-36 are rejected under 35 U.S.C. 103(a) as being  
unpatentable over Waldin, U.S. Patent No. 6,094,731, in view of Tamaru, U.S. Patent No. 4,788,637.

20        As per claims 1,13, and 25, the applicant describes a computer program product with the  
following limitations which are met by Waldin in view of Tamaru:  
  
a) reading logic operable to read an update status field associated with a computer file to be  
scanned by a current malware scanner, said update status field being indicative of an update status of a  
25 previous malware scanner that has scanned said computer file and associated said update status field  
with said computer file (Waldin: Col 6, lines 25-36);  
  
b) comparison logic operable to compare said update status of said previous malware scanner  
with an update status of said current malware scanner (Waldin: Col 6, lines 25-36);  
  
c) alert issuing logic operable if said update status of said current malware scanner does not  
30 match said update status of said previous scanner to issue an update status alert indicative of an out-of-

Art Unit: 2137

date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status (Tamaru: Figs 6 and 7);

Waldin describes a system similar to the applicant's in which an originating computer (2 of Fig 1) sends a file to a recipient computer (11 of Fig 1) over a network (14 of Fig 1). The file is a combination of 5 a data file (1 of Fig 1), a digital signature (15 of Fig 1), and an update file (4 of Fig 1) made up of update status fields including the version # of the previous scanner which scanned the file and the date virus definitions were last updated to the previous scanner. When the recipient computer receives the combined file, it reads the update file and compares the update status of the previous scanner with the update status of the current scanner. If the version # or date virus definitions were last updated to the 10 previous scanner are different from the version # or date virus definitions were last updated to the current scanner, the accelerator module (5' of Fig 1) alerts the current scanner (3' of Fig 1) to reexamine the file.

Waldin, however, does not disclose "an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and previous malware scanner has a most out-of-date update status". In other words, Waldin does not disclose a means to communicate to the 15 originating computer that he has an old version of a scanning program. Tamaru discloses a system between an originating computer and a recipient computer in which a message is sent between the two computers which includes a header indicating the version of a program the sending computer is using. The recipient computer compares the version with the version it is currently using and sends an alert indicative of whichever computer has the most outdated version of the program.

Fig 6 of Tamaru illustrates a situation in which station 2 has a more outdated version of a 20 program. Station 1 sends station 2 a message with a header indicating the version # of the program. In response to the message, station 2 sends station 1 an alert message indicating that station 2 has the most out-of-date status of the program. Fig 7 illustrates a situation in which station 1 has a more outdated version of a program. Station 1 sends station 2 a message indicating the version # of the 25 program. In response to the message, station 2 sends station 1 an alert indicating that station 1 has the most out-of-date status of the program.

Art Unit: 2137

Combining Tamari with Waldin would be easy. Waldin already has a means to determine the most out-of-date status of the scanner programs since it receives the date virus definitions were last updated in the originating computer and the version number of the scanner of the originating computer. When the comparison logic reveals that the update status of the previous scanner and the current 5 scanner are not the same and an alert is issued to the current scanner (3' of Fig 1) by the antivirus accelerator (5' of Fig 1), an alert indicative of whichever scanner has the most out-of-date status could also be issued by the antivirus accelerator to the originating computer as described by Tamari. Such an alert would allow the originating computer to know that its scanner program is outdated.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to 10 combine the ideas of Tamari with those of Waldin because doing so allows the originating computer to know if it has an outdated scanner program so that it can find a means to retrieve a newer program.

As per claims 2,14, and 26, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamari (see above), with the following limitation which is met 15 by Waldin:

Wherein said update status field is included as a property field within said computer file (Col 5, lines 21-27);

The property field is the header field.

20 As per claims 3-4,15-16, and 27-28, the applicant describes the limitations of claims 1,13, and 25, which are met by Waldin in view of Tamari (see above), with the following limitation which is met by Waldin:

Wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners (Col 5, lines 21-27).

25

As per claims 5,17, and 29, the applicant describes the limitations of claims 4,16, and 28, which are met by Waldin in view of Tamari (see above), with the following limitation which is met by Waldin:

Art Unit: 2137

Wherein said combined file is a file compressed combination of said update status file and said computer file (Col 6, lines 1-9);

The update status file is compressed by hashing and the hash is combined with the computer file to form a compressed combination of the update status file and the computer file.

5

As per claims 6, 18, and 30, the applicant describes the computer program product of claims 1, 13, and 25, which are met by Waldin in view of Tamari (see above), with the following limitation which is met by Tamari:

Wherein, if said malware scanner has a less out-of-date update status than said previous  
10 malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner (23 of Fig 2; Col 2, line 65 to Col 3, line 7);

The update status field is the version number. If current station 2 has a more recent program than station 1, the update status field (23 of Fig 2) is changed to correspond to the current station 2's program. The applicant should note that though Tamari specifically references a communication control  
15 program and the applicant references a scanner, the particular type of program is an obvious change in the system.

As per claims 8, 20, and 32, the applicant describes the limitations of claims 1, 13, and 25, which are met by Waldin in view of Tamari (see above), with the following limitation which is met by Tamari:

20 Wherein said update status alert includes one or more of:

a) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

b) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status (3 of Fig 1);

25 The administrator can be the controller of the stations.

Art Unit: 2137

As per claims 9,21, and 33, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamaru (see above), with the following limitation which is met by Waldin:

Wherein said computer file is an e-mail attachment (Col 5, lines 21-27).

5

As per claims 11,23, and 35, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamaru (see above), with the following limitation which is met by Waldin:

Wherein said update status field includes one or more of:

10 (i) a malware scanner computer program product identifier;  
(ii) a computer hardware identifier;  
(iii) a scanner engine program version identifier (Col 6, lines 31-36);  
(iv) a malware definition data version identifier.

15 As per claims 12,24, and 36, the applicant describes the computer program product of claims 1,13, and 25, which are met by Waldin in view of Tamaru (see above), with the following limitation which is met by Waldin:

Wherein said malware scanner server to detect one or more of:

20 (i) a computer virus (Col 2, lines 6-7);  
(ii) a Trojan computer program;  
(iii) a worm computer program;  
(iv) a banned computer program.

Claims 7,19, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waldin in  
25 view of Tamaru in further view of Cozza, U.S. Patent No. 5,502,815.

Art Unit: 2137

As per claims 7,19, and 31, the applicant describes the computer program product of claims 6,18, and 30, which are met by Waldin in view of Tamaru (see above), with the following limitation which is met by Cozza:

Wherein changes to said update status field are logged in an update status tracking database (20  
5 of Fig 2; Col 4, line 59 to Col 5, line 7);

Waldin in view of Tamaru disclose all the limitations of claims 7,19, and 31. However, Waldin in view of Tamaru fail to disclose the use of a database for logging changes to the update status fields.

Cozza discloses a system in which a scan information cache serves as a database for storing cache files which contain information about previous scans. When a new scan occurs, the cache files are updated.

10 It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Cozza with those of Waldin in view of Tamaru and add the use of a database because doing so allows an administrator or user to track changes to a system.

Claims 10,22, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waldin in  
15 view of Tamaru in further view of Grupe, U.S. Patent Application Publication No. 2002/0194487.

As per claims 10,22, and 34, the applicant describes the method of claims 1,13, and 25, which are met by Waldin in view of Tamaru (see above), with the following limitation which is met by Grupe:

Wherein said current malware scanner and said previous malware scanner are part of a tiered  
20 malware scanner [0017];

Waldin in view of Tamaru disclose all the limitations of claims 1,13, and 25. However, Waldin in view of Tamaru fail to disclose that the scanning environment is tiered.

Grupe discloses a similar scanning system which takes place in a tiered environment. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the  
25 ideas of Grupe with those of Waldin in view of Tamaru and incorporate the use of a tiered environment in the case where different computers have different scanning responsibilities.

Art Unit: 2137

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

5 Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through  
10 Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL  
SUPERVISORY PATENT EXAMINER

15 \*\*\*